

Testimony of Glenn S. Podonsky
Director, Office of Security and Safety Performance Assurance
U.S. Department of Energy
Before the
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives
March 14, 2006

Mr. Chairman and members of the Subcommittee, thank you for inviting me to testify regarding the Department of Energy's policies and practices for the protection of sensitive unclassified information, particularly as they relate to the information contained in the Government Accountability Office (GAO) Draft Report number GAO-06-369, "Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved." Classified and other sensitive information are among the national security-related and other government assets in our custody that we rigorously protect in accordance with the requirements of law, regulations, and national policies. We take our responsibilities in this area seriously, as we do our responsibilities to protect other national assets and interests. After reviewing the GAO draft report, the Department agreed that the findings contained in the draft report were accurate and fully concurred with all the report's recommendations. Before I discuss the issues of specific interest to the Subcommittee, I would like to briefly describe my office's responsibilities in this area.

The Office of Security and Safety Performance Assurance has a broad range of responsibilities associated with protecting information within the Department. These include: developing Department-wide information protection policies addressing the identification, marking, and protection of classified information and the various categories of sensitive unclassified information; conducting formal document control and protection training at our National Training Center; providing technical assistance to individual sites to improve their information protection programs; and providing independent oversight to determine the effectiveness of

information protection programs and practices throughout the Department. While Federal and contractor line managers at all levels in the Department are responsible for ensuring that our information is properly protected, my office provides policies and training to assist them, and provides oversight to ensure effective implementation.

DOE's Management of Sensitive Unclassified Information

The Subcommittee has asked me specifically to address our policies and practices for managing Official Use Only information, including the effectiveness of our training programs in assuring the identification and protection of sensitive records in accordance with established criteria. Congress, through the Freedom of Information Act (FOIA), has provided for public access to agency records upon request. Acknowledging that for a variety of reasons some categories of information need to be protected from public disclosure, Congress, in that same Act, established the authority and basis for exempting some information from public disclosure.

As a direct result of a recommendation made by the Commission on Science and Security (the Hamre Commission), in 2003 the Department established its first uniform agency-wide process for identifying and protecting sensitive information that we call Official Use Only information. This information is defined as unclassified information that has the potential to damage governmental, commercial, or private interests, and which may be exempt from public release under the FOIA. Prior to 2003, various Departmental elements had established internal processes and procedures for handling sensitive unclassified information referred to by various designations, including Official Use Only, but they did not apply agency-wide and were not standardized. In 2003 the Department issued a series of policy and implementation guidance documents – including an Order, a Manual, and a Guide – that formally established a uniform Department-wide program for identifying and protecting Official Use Only information. The purpose of our Official Use Only program is to: provide a means to control sensitive unclassified information and protect it from inappropriate disclosure; limit information protected from disclosure to that which is legally exempt under the FOIA; provide guidance for consistent and accurate identification of Official Use Only information; standardize the identification, marking

and protection of Official Use Only information; and facilitate the appropriate sharing of unclassified information.

The first thing I'd like to explain about the Official Use Only program is how an Official Use Only determination is made. There are two primary criteria for making an Official Use Only determination. The first criterion is whether or not the information has the potential to damage governmental, commercial, or private interests if released to persons who do not require it to do their jobs or other DOE-authorized activities. The second criterion is whether or not the information may fall under a FOIA exemption. I want to emphasize that an Official Use Only designation merely alerts individuals in possession of the information that it is sensitive, that it must be adequately controlled and protected, and that it must be reviewed prior to release – it does not mean that the information is automatically exempt from disclosure if requested under the FOIA. If the information is requested, the determination as to whether it can be released is made by an FOIA Authorizing or Denying Official based on a formal review.

Employees can determine that an unclassified document contains Official Use Only information if the employee's office has cognizance over the document – that is, if the document originated in their office, was produced for their office, or is under the control of their office. An Official Use Only determination is either based on formal guidance promulgated by a program office or made by an employee using the criteria of potential damage and the requirements of the FOIA.

Formal guidance can be issued in a variety of formats. Classification guides, in some instances, contain specific guidance for making Official Use Only determinations. For example, certain operational information, such as routine protective force deployment plans for facilities that do not possess Category I quantities of Special Nuclear Material is protected as Official Use Only. In the absence of guidance, an employee may make a determination based on the two criteria. While no formal certification is required to make Official Use Only determinations, the information necessary to guide decision-making for such determinations is available in Departmental-wide policy and guidance, program office policy and guidance, and various forms of local information security training.

If information is determined to be Official Use Only, the document or other medium in or on which it is contained must be appropriately marked. In addition to the obvious Official Use Only page markings, the first page must contain a marking identifying the FOIA exemption category that may be applicable, the requirement for review prior to public release, the name of the person making the determination, the date of determination, and any applicable guidance upon which the determination was based. In short, our system requires personnel to be accountable for their Official Use Only decisions.

Access to Official Use Only information is not overly restrictive. Official Use Only information may be provided to individuals – inside or outside of the Department – that need the information to perform their job or other DOE-authorized activity. Since Official Use Only information is not classified, a security clearance is not required; the only requirement is a need to know.

We require reasonable precautions for the protection of Official Use Only information. For example, it must be stored in secure buildings or in locked containers such as filing cabinets, desk drawers, or briefcases. We also require reasonable but simple precautions when reproducing, mailing, destroying, and electronically transmitting Official Use Only information, all aimed at ensuring the information is available only to authorized persons.

An Official Use Only determination is not necessarily permanent or irreversible. There are several ways in which Official Use Only information can be decontrolled. For example, the employee who made the original determination, or that employee's supervisor, may reevaluate the information and determine that it is not, or is no longer, Official Use Only. A program office may determine that certain program-related information is no longer Official Use Only and revise its guidance accordingly. Finally, upon a review resulting from a FOIA request for the information, a FOIA Authorizing Official may determine that the information may be released to the public.

Overall, our Official Use Only program is intended to provide a formal, workable process to identify, control, and protect certain sensitive unclassified information while making that information readily available for legitimate use. While we believe our program is effective in

helping us meet these goals, the GAO identified several areas that can be improved. As previously stated, we found the report to be a fair evaluation of our program and the findings to be accurate, and we fully concur with all recommendations.

The first recommendation is to clarify our guidance regarding the point in time at which a document should be marked as Official Use Only and to define inappropriate uses of the Official Use Only designation. Our response is to revise our Order and Manual to address these two points.

The second recommendation is to assure that all employees authorized to make Official Use Only determinations receive appropriate training before they make such determinations. Providing appropriate Official Use Only program training has been and remains the responsibility of line managers at the local level, with support and guidance from cognizant Headquarters organizations. Admittedly the form and content of that training has varied widely from location to location within the Department. As a result we are going to revise our program directives to require specific initial and refresher training, clearly identify the scope and content of that training, and assign responsibilities for ensuring that the training is developed and conducted.

The final recommendation is to conduct periodic oversight of Official Use Only program implementation. Our response is to develop a process to evaluate the identification, marking, and protection of Official Use Only information and incorporate that process into our Independent Oversight Program. We will also modify our policy directives to require the incorporation of similar evaluations into line management field oversight and local self-assessment activities. These actions will provide formal program oversight at several levels, and we believe will achieve the results the GAO is seeking.

Historical Records Review at National Archives and Records Administration

The Subcommittee has asked that I also address the Department's ongoing Congressionally-mandated effort to review documents released to the National Archives and Records Administration (NARA) by other agencies.

Under the Atomic Energy Act, the Department of Energy (DOE) controls the dissemination and declassification of Restricted Data, which can be loosely defined as nuclear weapon design, nuclear material production, and naval reactor information. We have dual responsibility, with the Department of Defense, for Formerly Restricted Data, which is information concerning the military utilization of nuclear weapons.

In 1995, when President Clinton signed Executive Order (EO) 12958, *Classified National Security Information*, it contained a key provision for the automatic declassification of National Security Information records of permanent historical value that were 25 years old or older, except for those documents that fell within certain specific exempt categories. Under EO 12958, the DOE and other agencies reviewed and released records which were then processed by NARA and placed on the open shelves where they were available to the public.

In 1996, Congress, concerned that DOE documents subject to the automatic declassification provisions of EO 12958 might contain Restricted Data, passed Public Law (PL) 104-106, which required the page-by-page review of DOE documents prior to release. Subsequently, Congress passed Section 3161 of the National Defense Authorization Act for Fiscal Year 1999 (PL 105-261), known as the Kyl Amendment, which required the DOE to develop a plan to prevent the inadvertent release of Restricted Data and Formerly Restricted Data through other agency records. The resulting plan, the Special Historical Records Review Plan, coordinated with NARA and the Information Security Oversight Office (ISOO), requires all departments and agencies to review their records page by page with reviewers trained by the DOE to recognize Restricted Data and Formerly Restricted Data, unless the records are highly unlikely to contain Restricted Data and Formerly Restricted Data. Since 1999, the DOE has trained over 2,000

Federal and contractor employees of other Government agencies to recognize Restricted Data and Formerly Restricted Data.

These programs ensured documents were reviewed by trained personnel prior to their release, but did not address documents already declassified and available to the public. The subsequent Lott Amendment (PL 106-65, Section 3149) applied the requirements of the Kyl Amendment to records already processed by NARA and the other agencies, including records that had already been made available to the public. The resulting Supplement to the Special Historical Records Review Plan, again coordinated with NARA and ISOO, required the DOE to survey records on the open shelves in order to identify those that were likely to contain Restricted Data or Formerly Restricted Data. Based on this mandate, we surveyed 213 million pages and withdrew thirty-seven million pages for audit examination. To date, we have returned approximately 35 million pages to the open shelves after NARA removed the documents that DOE identified as containing Restricted Data and Formerly Restricted Data. The approximately 2 million pages remaining are scheduled to be complete by the end of 2006.

Because the reclassification of documents is of particular concern to the Subcommittee, I would like to take a moment to address the issue. During our review of records at NARA, we have never reclassified information that was declassified. The Restricted Data and Formerly Restricted Data information that we found was classified at the time the Executive Order was issued and remains classified. We have, therefore, simply ensured that these documents are properly marked and protected as Restricted Data or Formerly Restricted Data. Our program was developed in close coordination with NARA.

Since 2000, we have submitted 20 reports to Congress (Committees on Armed Services) and the National Security Council (Assistant to the President for National Security Affairs) regarding the inadvertent release of Restricted Data and Formerly Restricted Data under EO 12958, which detail the ongoing findings of our reviews. Examples of classified information that we have identified during these reviews include information related to nuclear weapon design, special nuclear material production, radiological warfare, military utilization of nuclear weapons, and

Naval Nuclear Propulsion Information. We redact these reports to remove classified information and make the unclassified copies available to the public.

Concluding Remarks

I want to assure the members of the Subcommittee that the Department earnestly strives to protect all sensitive information in our possession as required and permitted by applicable laws, regulations, and Executive Orders. In determining how to protect information, as in determining how to protect our other national security assets, we apply a graded approach. That is, more valuable (or harmful to national security interests should it fall into the wrong hands) information is afforded a greater and more restrictive level of protection than is information of lesser value. Our Official Use Only program is designed to provide a prudent and reasonable level of protection to sensitive unclassified information while still accommodating our own and other's needs to use that information to conduct business, and to address as well the legitimate and recognized needs of the public to have access to that information. We believe our responses to the GAO recommendations will strengthen our program's ability to achieve those goals.

Thank you.